Illumio Segmentation

Contrôlez les déplacements latéraux pour éviter que les compromissions et les attaques par ransomware ne deviennent des incidents majeurs.

Segmentation moderne pour les réseaux d'aujourd'hui

Les réseaux tentaculaires, hybrides et en constante évolution d'aujourd'hui réunissent les conditions parfaites pour lancer des attaques.

Au cours de la seule année dernière, 88 % des entreprises ont été victimes de ransomwares et 58 % d'entre elles ont été contraintes d'interrompre leur activité à la suite de ces attaques.

Dans un monde caractérisé par les environnements multicloud hybrides, le télétravail et les applications distribuées, force est de constater que les périmètres traditionnels ont disparu depuis longtemps.

Une fois infiltrés, les cybercriminels peuvent se propager rapidement au sein de votre réseau et infecter silencieusement les systèmes et données critiques. Ce type de déplacement latéral est difficile à détecter, ce qui contribue à l'augmentation des compromissions, mais aussi à leur sophistication et à leur potentiel de destruction.

Les experts en cybersécurité reconnaissent qu'une approche Zero Trust basée sur la segmentation est le moyen le plus efficace pour confiner les compromissions, réduire les risques et renforcer la résilience.

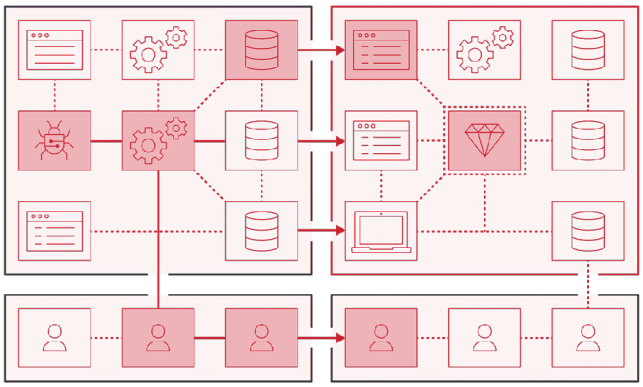
Illuminio Segmentation vous offre le contrôle nécessaire pour bénéficier d'une visibilité granulaire sur le trafic réseau, corriger les vulnérabilités, bloquer les déplacements latéraux non autorisés et confiner les compromissions — dans le cloud, les centres de données ou sur les terminaux.

Principaux avantages

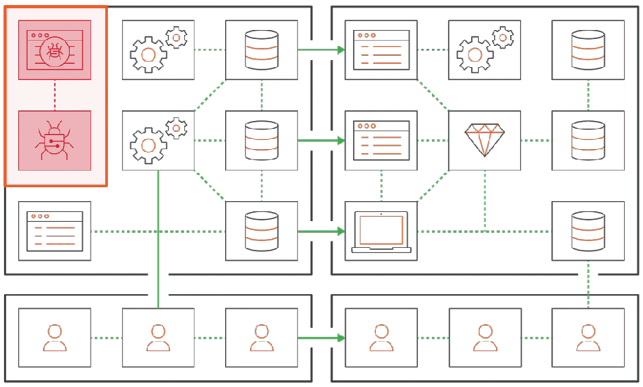
Visibilité granulaire complète
Cartographiez les communications associées aux charges de travail. Mettez au jour les risques cachés, puis créez des stratégies qui bloquent automatiquement les trajets habituels des ransomwares pour éviter toute propagation.

Segmentation simplifiée
Segmentez toutes les charges de travail exécutées dans le cloud, sur les terminaux et dans les centres de données. Empêchez la propagation des compromissions. Isolez les systèmes compromis. Bénéficiez d'une segmentation qui évolue en fonction des besoins de votre entreprise.

Le Zero Trust en toute simplicité
La segmentation est la base de toute stratégie Zero Trust. Appliquez le principe du moindre privilège. Éliminez la confiance implicite dans les environnements multicloud hybrides.



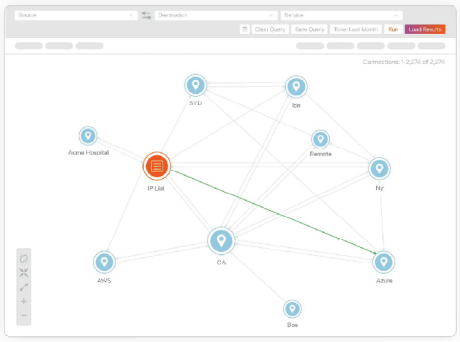
Sans segmentation, les compromissions se propagent rapidement.

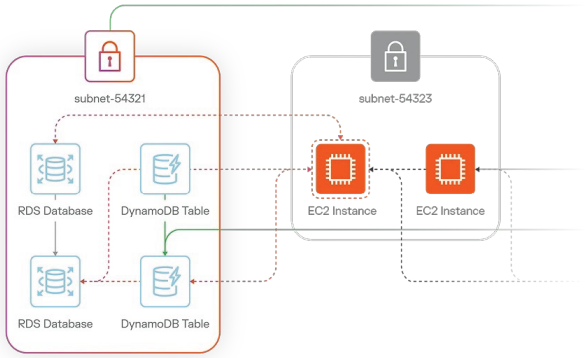


Avec segmentation, elles sont rapidement détectées et confinées.

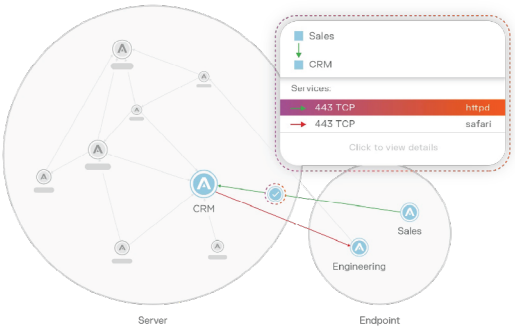
Une solution de segmentation pour chaque environnement

Quel que soit l'emplacement de vos charges de travail — dans le cloud, les centres de données ou sur les terminaux —, Illumio Segmentation vous offre une solution simple, cohérente et évolutive. Dites adieu aux outils cloisonnés et offrez-vous une sécurité Zero Trust unifiée, adaptée à tout votre environnement.





Confinez les attaques cloud à la source. Visualisez les applications, ressources, flux de trafic et métadonnées de votre cloud. Implémentez une segmentation cohérente et dynamique dans les conteneurs et environnements multicloud.



Confinez les compromissions sur un seul poste de travail, ordinateur portable ou machine virtuelle, avant même que celles-ci soient détectées par d'autres outils de sécurité. Visualisez le trafic des communications des terminaux et des applications au sein de votre réseau et appliquez le principe du moindre privilège.

Confinez les compromissions dans les centres de données locaux, les conteneurs, les environnements IT/OT et les machines virtuelles. Bénéficiez d'une visibilité complète sur tout le trafic, quelle que soit l'architecture, la taille ou la complexité de votre réseau. Segmentez les charges de travail sans interrompre les opérations.

Tirez parti de notre graphe de sécurité optimisé par l'IA

La plateforme Illumio repose sur un graphe de sécurité optimisé par l'IA qui offre une vue inégalée en temps réel de votre surface d'attaque. Illumio Insights et Illuminio Segmentation fonctionnent conjointement pour vous offrir une plateforme complète de confinement des compromissions.

Illumio Insights offre une solution cloud de détection et réponse (CDR) optimisée par l'IA qui identifie les risques, détecte les attaques et confine les menaces de façon instantanée, à l'échelle du cloud. Illuminio Segmentation vous aide à visualiser rapidement les risques et à appliquer des stratégies pour éviter la propagation des compromissions.

Confinez les compromissions avec Illumio Segmentation

illumio.com/fr/illumio-segmentation

À propos d'Illumio

Leader du confinement de ransomwares et de compromissions, Illumio redéfinit la façon dont les entreprises bloquent les cyberattaques et renforcent la résilience opérationnelle. Optimisée par un graphe de sécurité basé sur l'IA, notre plateforme de confinement des compromissions identifie et confine les menaces dans les environnements multicloud hybrides pour empêcher la propagation des menaces avant qu'elles ne donnent lieu à des incidents majeurs.

Classé parmi les leaders du rapport Forrester Wave™ sur les solutions de microsegmentation, Illumio favorise l'implémentation du modèle Zero Trust et renforce ainsi la cyberrésilience de l'infrastructure, des systèmes et des entreprises qui font tourner le monde.

Copyright © 2025 Illumio, Inc. Tous droits réservés. Illumio® est une marque commerciale ou marque commerciale déposée d'Illumio, Inc. ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Les marques commerciales tierces mentionnées dans le présent document appartiennent à leurs propriétaires respectifs.

Illumio Insights

Une solution cloud de détection et réponse reposant sur un graphe de sécurité optimisé par l'IA

Il est impossible de sécuriser ce que vous ne voyez pas

Au vu de la dépendance croissante des entreprises vis-à-vis des technologies cloud, il est important d'adopter une approche plus proactive de la sécurité. En d'autres termes, il est impératif de visualiser les vecteurs d'attaque potentiels et de prioriser les menaces à haut risque.

Sans cela, les équipes de sécurité peuvent être submergées d'alertes, incapables d'identifier les problèmes les plus critiques, et éprouver des difficultés à garder une longueur d'avance sur les compromissions.

- **De nombreuses attaques passent encore inaperçues.** Près de la moitié des entreprises déclarent être dans l'impossibilité d'identifier et de confiner rapidement les cyberattaques.
- **Garantir la sécurité des environnements cloud est plus complexe que jamais.** Les systèmes cloud ne cessent d'évoluer, ce qui complique singulièrement leur supervision.

Il est urgent de sécuriser le cloud. Au cours des dernières années, 98 % des entreprises ont été victimes de compromissions de données dans le cloud. Les méthodes de sécurité traditionnelles ont peine à suivre le rythme des environnements hybrides en constante évolution d'aujourd'hui.

Illumio Insights comble cette faille. Conçu pour l'échelle du cloud, Illumio Insights aide les équipes de sécurité à détecter les risques et à y remédier rapidement.

- **Bénéficiez d'une observabilité complète, en temps réel.** Cartographiez votre surface d'attaque multicloud hybride et analysez les risques en temps réel.
- **Identifiez et bloquez les déplacements latéraux.** Bénéficiez de données de flux et de contexte plus précises, qui montrent les déplacements possibles des cybercriminels entre les ressources cloud.
- **Simplifiez la détection et priorisez les réponses.** Conçu pour l'hyperscale, Illumio Insights gère les volumes considérables du trafic cloud à partir d'une plateforme centralisée afin que vous ayez accès aux informations critiques plus rapidement.

Principaux avantages

Observabilité complète

Bénéficiez d'un contexte complet sur l'ensemble des ressources, flux et charges de travail grâce à une classification et à un étiquetage optimisés par l'IA en quelques minutes à peine. Aucun matériel ni agent n'est nécessaire.

Détection plus intelligente des menaces

Transformez les données brutes du trafic en informations pertinentes et claires pour accélérer la détection et l'analyse des menaces. Repérez plus vite les menaces et prenez rapidement de meilleures décisions en matière de réponses.

Réponse priorisée

Identifiez et fermez de façon proactive les voies d'attaque à haut risque. Bloquez les déplacements latéraux en temps réel de façon réactive. Réduisez votre surface d'attaque.

Détection et réponse aux menaces fiables

Illumio Insights utilise l'IA pour aider les équipes de sécurité à détecter rapidement les menaces — en général, quelques minutes après l'installation. Il offre aux équipes une vue en temps réel des activités suspectes et montre les flux de trafic au sein des environnements, y compris les applications, les charges de travail, les rôles utilisateur et les fournisseurs cloud.

En combinant les données contextuelles et les informations sur les menaces optimisées par l'IA, les équipes de sécurité peuvent accélérer la traque des menaces et prendre des décisions plus avisées. Réduisez les risques et éliminez les menaces potentielles avec assurance.

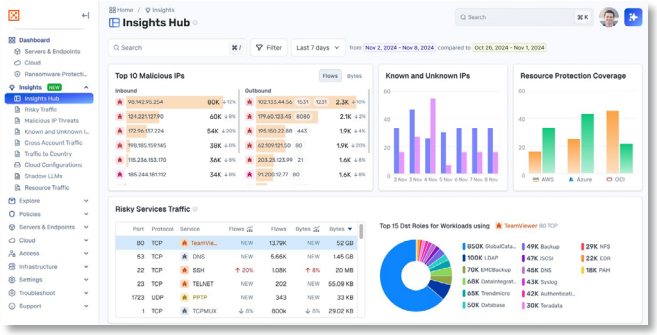
Document diffusé par MIEL

Fonctionnement

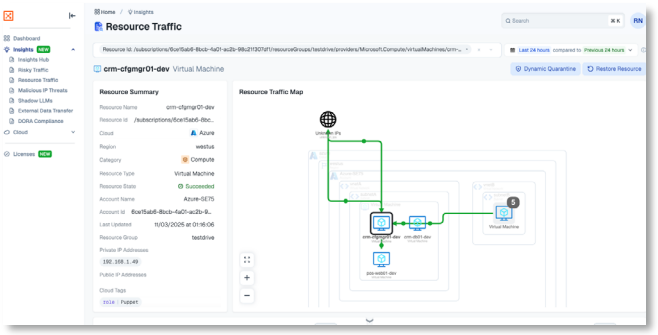
Illumio Insights est la première solution cloud de détection et réponse (CDR) basée sur un graphe de sécurité optimisé par l'IA. Composant essentiel de notre plateforme de confinement des compromissions, Illumio Insights peut observer et protéger toutes les charges de travail et ressources hébergées dans les environnements multicloud et hybrides.

Illumio Insights visualise le trafic et les comportements dangereux, et priorise les risques de déplacement latéral dans l'ensemble des environnements, afin d'aider les équipes à détecter et à réagir rapidement en cas de compromission.

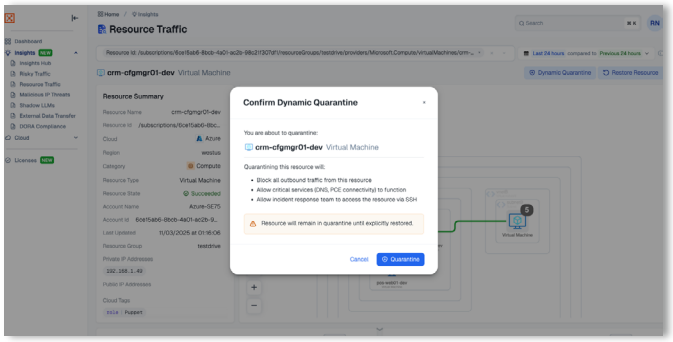
Installation simple et rapide à l'échelle du cloud. Bénéficiez d'informations optimisées par un graphe de sécurité d'IA sur des millions de charges de travail en quelques minutes, grâce à un déploiement sans agent en quelques clics.



Détection inégalée des menaces. Grâce à l'observabilité optimisée par l'IA, mettez plus rapidement au jour les menaces cachées et les voies d'attaque. Réduisez considérablement le délai moyen de détection (MTTD) des compromissions.



Confinement des compromissions en un clic. Neutralisez immédiatement les risques potentiels et réduisez le délai moyen de réponse (MTTR) aux compromissions.



Notre graphe de sécurité d'IA

Illumio Insights et Illuminio Segmentation sont deux composants clés de la première plateforme de confinement de compromissions reposant sur un graphe de sécurité optimisé par l'IA.

Illumio Insights aide les entreprises à accélérer l'identification des risques, la détection des attaques et le confinement des menaces en un seul clic. Elle offre aux équipes de sécurité les moyens de protéger les ressources critiques et d'intervenir sans délai. Illumio Insights et Illumio Segmentation fonctionnent conjointement pour identifier et limiter les risques, confiner les attaques et renforcer votre cyberrésilience.

Découvrez ce que vous avez manqué

Bénéficiez de la visibilité requise pour confiner les compromissions.

illumio.com/fr/illumio-insights

À propos d'Illumio

Leader du confinement de ransomwares et de compromissions, Illumio redéfinit la façon dont les entreprises bloquent les cyberattaques et renforcent la résilience opérationnelle. Optimisée par un graphe de sécurité basé sur l'IA, notre plateforme de confinement des compromissions identifie et confine les menaces dans les environnements multicloud hybrides pour empêcher la propagation des menaces avant qu'elles ne donnent lieu à des incidents majeurs.

Classé parmi les leaders du rapport Forrester Wave™ sur les solutions de microsegmentation, Illumio favorise l'implémentation du modèle Zero Trust et renforce ainsi la cyberrésilience de l'infrastructure, des systèmes et des entreprises qui font tourner le monde.

Copyright © 2025 Illumio, Inc. Tous droits réservés. Illumio® est une marque commerciale ou marque commerciale déposée d'Illumio, Inc. ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Les marques commerciales tierces mentionnées dans le présent document appartiennent à leurs propriétaires respectifs.